JC05 Rec'd PCT/PTO 13 APR 2001

FORM PTO-1390 (REV. 1094) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		B1039/7001 (LMG)
		U S APPLICATION NO (If known, see 37 CFR 1.5) 09/807482
INTERNATIONAL APPLICATION NO. PCT/NZ99/00176	INTERNATIONAL FILING DATE 15 October, 1999 (15.10.99)	PRIORITY DATE CLAIMED 16 October, 1998 (16.10.98)

TITLE OF INVENTION
REMOTE ACCESS AND SECURITY SYSTEM

APPLICANT(S) FOR DO/EO/US
Kenneth Edwin THOMAS et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [x] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [x] This express request to begin national procedures (35 U.S.C. 371(f) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [x] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [x] A copy of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [x] has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)) with drawings.

7. [x] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)).
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. [x] have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(C)(5)).

Items 11. To 16. Below concern document(s) or information included:

11. [x] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. [x] A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. [x] Other items or information:
    Copy of WO 00/23960, publication of International Application No. PCT/NZ99/00176

Express Mail Label No. EL 844532225US
Dated: April 13, 2001

JC02 Rec'd PCT/PTO 13 APR 2001

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 09/807482	INTERNATIONAL APPLICATION PCT/NZ99/00176	ATTORNEY'S DOCKET NUMBER B1039/7001 (LMG)

17. [x] The following fees are submitted:

	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO .....$860.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) .....$690.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)).....$710.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO.....$1,000.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4).....$100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1,000.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐20 ☐30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	22-20 =	2	X $18.00	$36.00	
Independent Claims	2- 3 =	0	X $80.00	$0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$270.00	$0	
TOTAL OF ABOVE CALCULATIONS =				$1036.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$1036.00	
Processing fee of $130.00 for furnishing the English translation later than ☐20 ☐30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$	
TOTAL NATIONAL FEE =				$1036.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate coversheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$1036.00	
				Amount to be: refunded	
				charged	$100.00

a. [x] A check in the amount of $936.00 to cover the above fees is enclosed.

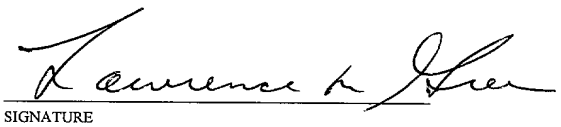
b. [x] Please charge my Deposit Account No. 23/2825 in the amount of $100.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [x] The commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 23/2825. A duplicate of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Lawrence M. Green, Esq.
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210



SIGNATURE

Lawrence M. Green
NAME

29,384
REGISTRATION NO

Form)T)-1390 (REV 10-94) page 2 of 2

527805.1

09/807482
JC02 Rec'd PCT/PTO 13 APR 2001

Express Mail No.: EL844532225US

ATTORNEY'S DOCKET NO: B1039/7001 (LMG)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Kenneth Edwin THOMAS et al.
International Application No.:	PCT/NZ99/00176
International Filing Date:	15 October, 1999
For:	REMOTE ACCESS AND SECURITY SYSTEM

Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to examination, please amend the above-identified application as follows:

IN THE CLAIMS:

Please cancel claims 23 and 24 without prejudice or disclaimer.

Kindly rewrite claims 3, 5, 8, 9, 11, 13, 14 and 18-20 as follows:

3. (Amended) A remote access control system as claimed in claim 1 wherein the access control data includes operator control unit identification data, operator identification data and access controller identification data.

5. (Amended) A remote access control system as claimed in claim 1 wherein the identity structure is encrypted and can only be deciphered by selected access controllers and the central control means.

8. (Amended) A remote access control system as claimed in claim 1 wherein the first communication means includes a wide area communications network.

9. (Amended) A remote access control system as claimed in claim 1 wherein the second communication means includes a wide area communications network.

11. (Amended) A remote access control system according to claim 1 wherein each access controller includes recordal means adapted to record data relating to the conditions or circumstances of its associated value unit.

13. (Amended) A remote access control system according to claim 11 wherein the data recorded is transferred to the central control means, via the virtual configuration link.

14. (Amended) A remote access control system according to claim 1 wherein each access controller includes a locking mechanism and an electronic control device.

18. (Amended) A method according to claim 15 wherein the first communication means includes a wide area communications network.

19. (Amended) A method according to claim 15 wherein the second communication means includes a wide area communications network.

20. (Amended) A method according to claim 15 wherein the second communication means includes a local communications link.

REMARKS

It is respectfully requested that the foregoing Preliminary Amendment be entered prior to examination of the application, to place the application in better condition for examination and allowance. No new matter has been added.

It is respectfully submitted that all of the claims in the application are in condition for allowance, and prompt and favorable consideration is hereby requested.

Respectfully Submitted,

Kenneth Edwin THOMAS et al., Applicants

Lawrence M. Green
Reg. No. 29,384
WOLF, GREENFIELD & SACKS, P.C.
600 Atlantic Avenue
Boston, MA 02210
Telephone: (617) 720-3500
Attorney for Applicants

Docket No.: B1039/7001
Date: April 13, 2001

MARKED-UP CLAIMS

3. (Amended) A remote access control system as claimed in [either] claim 1 [or claim 2] wherein the access control data includes operator control unit identification data, operator identification data and access controller identification data.

5. (Amended) A remote access control system as claimed in [any one of] claim[s] 1 [to 4] wherein the identity structure is encrypted and can only be deciphered by selected access controllers and the central control means.

8. (Amended) A remote access control system as claimed in [any one of the preceding] claim[s] 1 wherein the first communication means includes a wide area communications network.

9. (Amended) A remote access control system as claimed in [any one of the preceding] claim[s] 1 wherein the second communication means includes a wide area communications network.

11. (Amended) A remote access control system according to [any one of the preceding] claim[s] 1 wherein [the or] each access controller includes recordal means adapted to record data relating to the conditions or circumstances of its associated value unit.

13. (Amended) A remote access control system according to [either] claim 11 [or claim 12] wherein the data recorded is transferred to the central control means, via the virtual configuration link.

14. (Amended) A remote access control system according to [any one of the preceding] claim[s] 1 wherein [the or] each access controller includes a locking mechanism and an electronic control device.

18. (Amended) A method according to [any one of] claims 15 [to 17] wherein the first communication means includes a wide area communications network.

19. (Amended) A method according to [any one of] claim[s] 15 [to 18] wherein the second communication means includes a wide area communications network.

20. (Amended) A method according to [any one of] claim[s] 15 [to 18] wherein the second communication means includes a local communications link.

13 Rec'd PCT/PTO 13 APR 2001
09/807482

REMOTE ACCESS AND SECURITY SYSTEM

TECHNICAL FIELD

This invention relates to a remotely operable access and security system.

BACKGROUND

There are many circumstances in which it may be desirable for an owner, operator or manager of items of value to have control over access to that or those items wherever they may be and by whom.

There are many security systems available. In general such security systems may control who has access to the item of value, for example access to buildings or other sites to selected people, such as employees; access to safes, vaults and other such security containers; access to vehicles; access to information and data on a personal computer or a database. These are just a few examples.

In some circumstances existing security systems allow for remote operation of access to a fixed site. In other systems, such as electronically controlled alarms and locks on motor vehicles, the item of value is moveable, but access to it is only controllable at a local level and only by the pre-selected operator.

However, many circumstances exist where security is required in relation to an item or items which do not have a fixed location, and/or for which access is required by a range of different people, perhaps in different circumstances, and for which the owner/operator/manager will wish to retain control over who has access, where and when. To provide such flexibility, the lock may need to have different characteristics at different times or locations.

One system presently known which may be used to allow controlled access to a moveable item's location is to provide a programmable key which can communicate with the lock via a local area communications system. Such a system is described in United States patent specification No. US 4,766,746. The key is

programmed by an authorising person or system via a wide area communications network to enable it to open one or more locks, each of which may be identified by a unique identification number. A pin or access number may be required to verify that an authorised person has the key. The key then communicates with the lock, instructing it to open.

The key may also be programmed with information to reconfigure the characteristics of the lock, for example any time periods during which the lock will not open. This function provides increased functional flexibility to the lock and helps to avoid having to reprogram the lock at a central servicing location.

However, at present, security systems of this type require the operator to specifically program the lock. This requires someone to travel to the location of the local area communications system of the lock to enable communication with the lock to reconfigure it. This reconfiguring may be performed the next time someone wishes to enter the lock, but this person may not know how to reconfigure the lock. Alternatively, the person may forget to reconfigure the lock or may not be trusted to reconfigure the lock before accessing the items of value. Therefore, the reconfiguration may not occur, resulting in a risk of a security breach.

Another disadvantage of this method is that control intelligence relating to the lock is readable by the key and therefore may be susceptible to theft. This may compromise the security of the lock by, for example, allowing others to identify the times when the lock may be opened.

Furthermore, this type of system does not allow for simultaneous central control of access by a plurality of operators to a single value unit or site, or of access by one or more operators to multiple value units.

Other known methods of providing remote security locking include providing a direct communication link between the lock and the authorising person or system, as is described in United States patent specification No. US 5,815,557. The direct link has the advantage of ensuring that the lock can be reconfigured at any time. One method involves the person requiring to open the lock communicating their intention to the authorising person or system and

adequately identifying themselves. The authorising person or system then sends a signal to open the lock. Reconfiguration data may be sent directly to the lock via the communication link. This method has the disadvantage of requiring the authorising person or system to be available when access is required to send the command to open the lock.

Another known solution to the problem of providing remote security locking, again described in the United States patent specification No. 4,766,746, also involves having a direct communication link between the lock and the authorising person or system to provide configuring information and a second communication link between a key and the authorising person or system. The key receives a communication enabling it to open one or more locks and may require a PIN to ensure an authorised person is using the key. This method has the disadvantage of requiring the lock to be connected to a wide area communications network, increasing its cost and complexity and possibly limiting its portability.

Thus, it is an object of the present invention to provide a method and apparatus for enabling security for and/or access to items of value remotely that overcomes or alleviates problems in such methods and apparatus at present or at least to provide the public with a useful choice.

Other objects of the present invention may become apparent from the following description which is given by way of example only and with reference to the accompanying drawings.

SUMMARY OF THE INVENTION

According to one aspect of the present invention there is provided a remote access control system adapted to enable the remote control of access to one or more value units by one or more operators, the system including:

- a central control means including control data including an identity structure relating to the permissible behaviour of an access controller and access control data defining operator control over the access controller;
- one or more access controller, each adapted to selectively prevent or enable access to a value unit;
- one or more operator control unit, including actuating means, adapted to enable interaction of an operator with the control system;
- first communication means adapted to provide remote communication between the central control means and one or more operator control unit;
- second communication means adapted to provide remote communication between an operator control unit and one or more access controller;
- and wherein when communication of identity structure to an access controller unit is required, a virtual configuration link is created between the central control means and the access controller for that value unit, via an operator control unit, for the transfer of the identity structure from the central control means to the access controller to initialise the access controller and so allow the access control data to gain access to the access controller.

Preferably, the identity structure may include an application template and configuration data for the access controller.

Preferably, the access data may include operator control unit identification data, operator identification data and access controller identification data.

Preferably, the identity data, and optionally all the control data, may be encrypted, and at least the identity data may only be deciphered by selected access controllers and the central control means.

According to a further aspect of the invention there is provided a method of remotely controlling access to a value unit through a control system by an operator including:

- providing, at a central control means, access control data relating to the control of access to a value unit by an associated access controller;
- providing, at the central control means, an identity structure relating to the permissible behaviour of the access controller;
- operating an operator control unit via actuating means to interact with the control system;
- forming a virtual configuration link between the central control means and the access controller, via the operator control unit, for transfer of the identity structure from the central control means to the access controller via first communication means providing remote communication between the central control means and the operator control unit and second communication means providing remote communication between the operator control unit and the access controller, the identity structure initialising the access controller to allow the access control data to gain access to the access controller and therefore enable access to the value unit.

Other aspects of the present invention may become apparent from the following description which is given by way of example only and with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1:

Shows a diagrammatic representation of the operation of the system of the present invention.

Figure 2:

Shows an example of use of the system of the present invention in controlling access to shipping containers

DETAILED DESCRIPTION OF THE INVENTION

In this specification reference is made to centralised management nodes (CMNs) or central control means, personal access nodes (PANs) or operator control units and remote value nodes (RVNs) or access controllers. The term CMN is used to describe a database, management and communication system that supplies RVN identity structure, template and configuration data and access and control information to one or more PAN.

The term PAN is used to describe a personal access device which an authorised person can use to access one or more allocated RVN. Thus, a PAN will have some form of actuation means such as a portable keypad device, with communication means enabling it to communicate to the CMN and one or more RVN.

The term RVN is used to describe an electronic control device which is associated with any form of valuable item which requires controllable access. Examples of valuable items (hereafter referred to as "value units") would include shipping containers, retail security cabinets, vending machines, buildings, courier bags, and the like. These examples include locking mechanisms which may be remotely operated. It will be appreciated that there are many other types of value unit which may include locking mechanisms which could be controlled through the system of the present invention, such as personnel security access. In addition, the invention may be equally applicable to the control of access to different types of value unit, such as data and information, via security systems other than physical

locks. This may include, for example, internet access, smart card cash transfer, and access to electronic databases of any type.

A PAN provides an intermediate communication link between the CMN and one or more RVN. Communication between the CMN and the or each PAN is via, for example, direct serial link using local PC connections, one or two-way pager networks, a two-way cellphone network or other means of wide area data communication.

Communication between a PAN and one or more RVN is via local area communication means, such as an infrared link, a local area RF link or a direct connection.

A RVN may include a controller unit and an associated locking mechanism. For security reasons a RVN may be located within its associated value unit. For example, if the item is a shipping container or vending machine, then the RVN would be inside that container or machine, would preferably be communicated to by the PAN by remote means, and would therefore be inaccessible except via access to the value unit by an operator of the PAN.

Any given RVN controller has a programming means suitable to store and implement an identity structure. The nature of this identity structure will depend on the nature of the value unit controlled by the RVN. It could include, as a minimum, an access combination. It may also include: time and location criteria, if the item is one which may only be accessed at specific times or dates, or at specific locations (for example controlled by a GPS unit); control criteria, such as how often the unit may be accessed, how long the unit is accessible after access is provided; user/operator group access criteria; and encryption and decryption criteria.

An RVN controller may have a plurality of identity structures so that it may be adapted to operate in a number of different ways.

The identity structure is specific to each RVN application. Each application has an identity structure including a template that can be loaded with configuration data to suit a particular application; different applications being appropriate for different value units and in different circumstances.

The system of the present invention enables the controlled access to one or more RVN from the CMN by employing a virtual configuration link (VCL) between the CMN and the one or more RVN, via one or more PAN. The VCL allows the transfer of communication data between the CMN and RVN automatically when the PAN interfaces with the RVN.

Operation of the system of the present invention is now described in broad terms with reference to Figure 1.

Information is communicated within the system within three communication protocol layers, the access layer, identity layer and VCL layer. The system creates a secure virtual link as information communicated to the PAN from the CMN and from the PAN to the RVN remains inaccessible to the PAN access layer. The secure virtual link cannot be attacked in the PAN as the access layer does not have access to the encryption.

The access layer communicates security access and control data, which may include user interface, PAN identification, user identification, RVN identification and RVN access and control data. The access layer includes control of the remote value node to ultimately allow or prevent access to the value unit.

The identity layer controls and communicates information relating to the identity structures of the RVN. The CMN constructs the RVN identity structure which determines the behaviour of that RVN. As stated above, the RVN structure includes an application template and configuration data, and also includes initialisation instructions. Without the identity structure an RVN includes no information that would allow it to be vulnerable to "attack" or interference. If, for example, the RVN is an electronic lock on a container, the lock is a "virtual" lock until it is given an identity.

A secure VCL is created by encryption of the information in the identity structure layer. The information is only decipherable by the CMN and RVN and is transmitted as VCL data packets in the VCL by the CMN to the RVN.

The operation of the system of the present invention will now be described in broad terms.

Each PAN has a unique identification number. A PAN is "activated" by communication of its correct identification number to or from the CMN. Any given user or operator of a PAN has an access or PIN number. The CMN loads one or more user authorisations to the PAN in the form of the access or PIN number. The CMN then also loads to the PAN one or more identification numbers for one or more RVN which is to be accessed by the PAN at some time. Hence, a single PAN may be authorised to enable access to multiple RVN to a schedule. The identification numbers and access or PIN number are communicated as part of the access layer protocol. Communication between the CMN and PAN is accomplished via communication means #1 (see Figure 1).

An application template for the or each RVN is then created by the CMN as part of the identity layer protocol. Configuration data is then loaded based on the information specifying, for example, the PAN identification number, operator identification, RVN identification and operator entry combinations. The combined information communicated by the template and configuration data will vary depending on the application of the RVN.

The combined information is encrypted such that it can only be deciphered by the RVN. This creates a secure VCL between the CMN and the remote RVN as the PAN cannot decipher the encrypted information. The encrypted information is then downloaded to the PAN as a VCL data packet

Once all necessary data has been communicated from the CMN to the PAN, and a selected operator has correctly identified themselves to the PAN using their access or PIN number, the PAN communicates via communications means #2 (see Figure 1), which may comprise a local area communications link to the or each RVN. The PAN will download the VCL data packet to a correctly identified RVN.

The controller of the RVN deciphers this data, and makes it available to the identity layer in the RVN.

At the identity layer, the RVN reconstructs the application template and loads in the configuration data, then processes this data to initialise the access layer. The configuration data in the application template defines a set of parameters which dictate the operation of the RVN. It will be appreciated that a template may remain programmed into a RVN while the configuration data may be updated through the VCL. Alternatively, a new template and configuration data may be programmed into a RVN, through the VCL each time the RVN is accessed by the PAN.

It is an important feature of the present invention that the existence of a VCL between the CMN and RVN avoids the necessity of an operator to purposefully reconfigure the RVN. When reconfiguration is required, the required data defining the identity structure is simply communicated to one or more PAN; the new identity structure being programmed automatically into the RVN the next time a PAN communicates with the RVN.

The PAN also communicates to the RVN via the access layer, data which could include operator access and control codes. Also at the access layer, the RVN validates the information and permits access to the value unit.

It will be appreciated that each PAN may have one or more assigned operators and can be programmed to access one or more RVN. Each RVN may also allow access by more than one PAN, for example to allow multiple authorised people through a door to a building.

Access and control data is "known" to the PAN and may, for example, contain user identification/PIN numbers, the PAN identification number and access combination details.

A PAN establishes the VCL between the CMN and a RVN by creating a virtual security tunnel. The CMN encrypts the identity structure and creates VCL data packets. The PAN does not have access to the encrypted configuration information contained in the VCL data packets because it does not have the required

deciphering codes. When the PAN communicates with a remote RVN the VCL data packet information is downloaded to the RVN which then deciphers the information and updates the RVN template and configuration on the identity layer. The RVN can then process the user level access and control data, also communicated from the PAN.

The RVN may also store relevant information relating to its environment and conditions and communicate this information back to the CMN via a VCL established by a PAN. The information may include, for example, recordings of the air temperature around or within the RVN at various times, information relating to the time spent in any specific location or any other useful information which provides the owner/operator with a history of the circumstances of the unit. This information may be downloaded to the CMN via a PAN at the time of access.

An example of the system of the present invention in operation is now presented with specific reference to the control of access to a shipping container. It will be appreciated that shipping containers are a good example of a value unit which does not have a fixed location and which may need to be accessed at different times, in different places by a variety of different operators. It will also be appreciated that the present invention has application in numerous alternative circumstances as referred to previously.

A RVN controller may be located inside a shipping container for controlling the locking mechanism. There would be no physical connection between the RVN and the outside of the container, except for a communication means enabling communication between the controller and a PAN.

Reference is now made to Figure *2*. A remote shipping agent 1 requiring access to a container 2 at the port of destination would communicate their need to access the container to the local shipping agent or security manager 3. Alternatively, this communication may be unnecessary if the RVN in that container has been pre-programmed to enable access at specific locations and times.

SUBSTITUTE SHEET (RULE 26)

The local shipping agent or security manager authorises the remote agent to access a designated container by sending authorisation data to the PAN 4 via the CMN 5. This communication is shown as being via a locally linked PC connection 6 and a wide area communications network 7.

An activated PAN transfers configuration, access and control information to the relevant RVN and thus allows access to the container 2.

Thus, using a system of the present invention an owner/manager of value units which have no fixed location can provide security access to that or those items at any given time or place and only by authorised users/operators. The VCL provides a means for the CMN to communicate with a RVN to update its identity structure, ensuring that the identity structure is updated when required and avoiding the expense of a separate communication system. The unit itself has no fixed external keypad or means of direct communication with the PAN. Furthermore, control intelligence relating to a particular RVN is held in the CMN and not in the RVN itself. The identity structure need only be loaded to the RVN immediately before access is required and removed, if necessary, after access, so that there is no useful information in the RVN which could be vulnerable to attack. Additional security is provided by encryption of data to provide a secure VCL between the CMN and RVN.

Where in the foregoing description reference has been made to specific components or integers of the invention having known equivalents then such equivalents are herein incorporated as if individually set forth.

Although this invention has been described by way of example and with reference to possible embodiments thereof it is to be understood that modifications or improvements may be made thereto without departing from the scope or spirit of the invention.

CLAIMS

1. A remote access control system adapted to enable the remote control of access to one or more value units by one or more operators, the system including:

- a central control means including control data including an identity structure relating to the permissible behaviour of an access controller and access control data defining operator control over the access controller;

- one or more access controller, each adapted to selectively prevent or enable access to a value unit;

- one or more operator control unit, including actuating means, adapted to enable interaction of an operator with the control system;

- first communication means adapted to provide remote communication between the central control means and one or more operator control unit;

- second communication means adapted to provide remote communication between an operator control unit and one or more access controller;

- and wherein when communication of identity structure to an access controller unit is required, a virtual configuration link is created between the central control means and the access controller for that value unit, via an operator control unit, for the transfer of the identity structure from the central control means to the access controller to initialise the access controller and so allow the access control data to gain access to the access controller.

2. A remote access control system as claimed in claim 1 wherein the identity structure includes an application template and configuration data.

3. A remote access control system as claimed in either claim 1 or claim 2 wherein the access control data includes operator control unit identification data, operator identification data and access controller identification data.

4. A remote access control system as claimed in claim 3 wherein the access control data further includes data relating to the conditions for permissible access.

5. A remote access control system as claimed in any one of claims 1 to 4 wherein the identity structure is encrypted and can only be deciphered by selected access controllers and the central control means.

6. A remote access control system as claimed in claim 1 wherein the control data is encrypted.

7. A remote access control system according to claim 1 wherein the identity structure is inaccessible to an operator of an operator control unit.

8. A remote access control system as claimed in any one of the preceding claims wherein the first communication means includes a wide area communications network.

9. A remote access control system as claimed in any one of the preceding claims wherein the second communication means includes a wide area communications network.

10. A remote access control system as claimed in claim 8 wherein the second communication means includes a local communications link.

11. A remote access control system according to any one of the preceding claims wherein the or each access controller includes recordal means adapted to record data relating to the conditions or circumstances of its associated value unit.

12. A remote access control system according to claim 11 wherein the data recorded includes the conditions or circumstances of operator access.

13. A remote access control system according to either claim 11 or claim 12 wherein the data recorded is transferred to the central control means, via the virtual configuration link.

14. A remote access control system according to any one of the preceding claims wherein the or each access controller includes a locking mechanism and an electronic control device.

15. A method of remotely controlling access to a value unit through a control system by an operator including:

- providing, at a central control means, access control data relating to the control of access to a value unit by an associated access controller;
- providing, at the central control means, an identity structure relating to the permissible behaviour of the access controller;
- operating an operator control unit via actuating means to interact with the control system;
- forming a virtual configuration link between the central control means and the access controller, via the operator control unit, for transfer of the identity structure from the central control means to the access controller via first communication means providing remote communication between the central control means and the operator control unit and second communication means providing remote communication between the operator control unit and the access controller, the identity structure initialising the access controller to allow the access control data to gain access to the access controller and therefore enable access to the value unit.

16. A method according to claim 15 wherein the identity data is encrypted and can only be deciphered by selected access controllers.

17. A method according to claim 15 wherein the control data is encrypted.

18. A method according to any one of claims 15 to 17 wherein the first communication means includes a wide area communications network.

19. A method according to any one of claims 15 to 18 wherein the second communication means includes a wide area communications network.

20. A method according to any one of claims 15 to 18 wherein the second communication means includes a local communications link.

21. A method according to claim 15 further including recording of data relating to the conditions or circumstances of the value unit by the access controller and transferring this data to the central control means via the virtual configuration link.

22. A method according to claim 21 wherein the data recorded includes the conditions or circumstances of operator access of the value unit.

23. A remote access control system substantially as herein described and with reference to the accompanying drawings.

24. A method of remotely controlling access to a value unit substantially as herein described by way of example and with reference to the accompanying drawings.

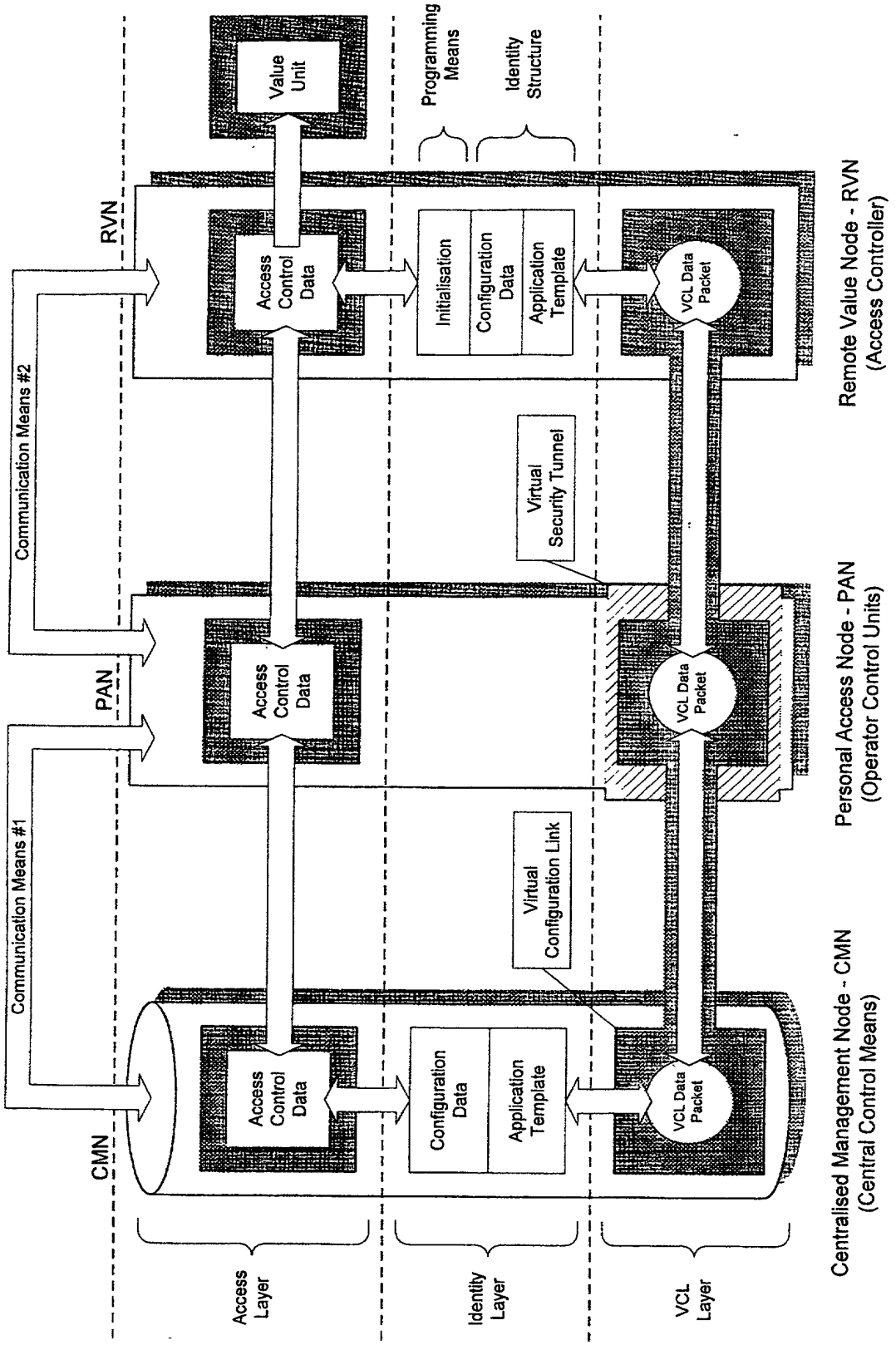

Value Unit
Programming Means
Identity Structure
RVN
Access Control Data
Initialisation
Configuration Data
Application Template
VCL Data Packet
Remote Value Node - RVN (Access Controller)
Communication Means #2
Virtual Security Tunnel
PAN
Access Control Data
VCL Data Packet
Personal Access Node - PAN (Operator Control Units)
Communication Means #1
Virtual Configuration Link
CMN
Access Control Data
Configuration Data
Application Template
VCL Data Packet
Centralised Management Node - CMN (Central Control Means)
Access Layer
Identity Layer
VCL Layer

FIGURE 1

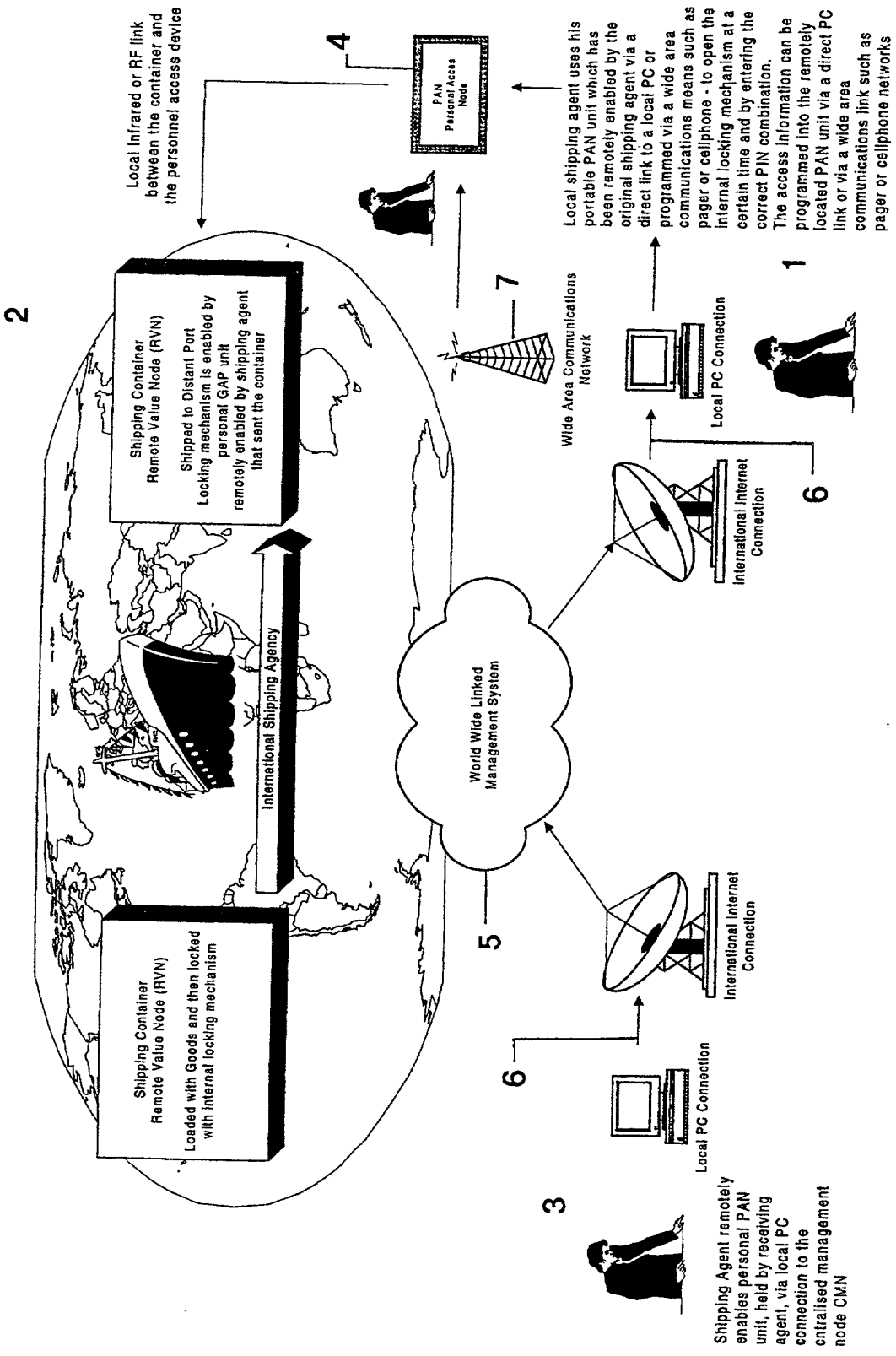

Local Infrared or RF link between the container and the personnel access device
4
PAN Personal Acess Node
Local shipping agent usss his portable PAN unit which has been remotely enabled by the original shipping agent via a direct link to a local PC or programmed via a wide area communications means such as pager or cellphone - to open the internal locking mechanism at a certain time and by entering the correct PIN combination.
The access information can be programmed into the remotely located PAN unit via a direct PC link or via a wide area communications link such as pager or cellphone networks
1
2
Shipping Container Remote Value Node (RVN)
Shipped to Distant Port
Locking mechanism is enabled by personal GAP unit remotely enabled by shipping agent that sent the container
International Shipping Agency
Shipping Container Remote Value Node (RVN)
Loaded with Goods and then locked with internal locking mechanism
7
Wide Area Communications Network
Local PC Connection
6
International Internet Connection
World Wide Linked Management System
5
6
Local PC Connection
International Internet Connection
3
Shipping Agent remotely enables personal PAN unit, held by receiving agent, via local PC connection to the centralised management node CMN

FIGURE 2

Attorney Docket No. B1039/7001

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

REMOTE ACCESS AND SECURITY SYSTEM

the specification of which is attached hereto unless the following is checked:

[X] International Application No. PCT/NZ99/00176, which was filed on October 15, 1999, and which entered the U.S. National Phase, as Application No. 09/807,482, bearing Attorney Docket No. B1039/7001 (LMG).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or section 365(a) of any PCT International application designating at least one country other than the United States listed below and have also identified below any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed:

Prior Foreign PCT International Application(s)and any priority claims under 35 U.S.C. §§119 and 365(a),(b):

(Number)	(Country-if PCT, so indicate)	(DD/MM/YY Filed)	Priority Claimed YES	NO
332374	New Zealand	16 October, 1998	[X]	[ ]
			[ ]	[ ]
			[ ]	[ ]

DOCKET NO. B1039/7001

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

(Application Number)	(filing date)
(Application Number)	(filing date)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s), or §365(c) of any PCT International application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application No.)	(filing date)	(status-patented, pending, abandoned)
(Application No.)	(filing date)	(status-patented, pending, abandoned)

PCT International Applications designating the United States:

(PCT Appl. No.)	(U.S. Ser. No.)	(PCT filing date)	(status-patented,pending,abandoned)

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Robert M. Abrahamsen	40,886	Jason M. Honeyman	31,624	Stanley Sacks	19,900
Eric Amundsen	46,518	Robert E. Hunt	39,231	Christopher S. Schultz	37,929
John N. Anastasi	37,765	Ronald J. Kransdorf	20,004	Alan B. Sherr	42,147
Ilan Barzilay	46,540	Peter C. Lando	34,654	Robert A. Skrivanek, Jr.	41,316
Gary S. Engelson	35,128	M. Brad Lawrence	P 47,210	Alan W. Steele	45,128
Neil P. Ferraro	39,188	Helen C. Lockhart	39,248	Mark Steinberg	40,829
Thomas G. Field, III	45,596	Matthew B. Lowrie	38,228	Joseph Teja, Jr.	45,157
Stephen R. Finch	42,534	William R. McClellan	29,409	John R. Van Amsterdam	40,212
Edward R. Gates	31,616	Daniel P. McLoughlin	46,066	Michael G. Verga	39,410
Richard F. Giunta	36,149	James H. Morris	34,681	Robert H. Walat	46,324
Peter J. Gordon	35,164	M. Lawrence Oliverio	30,915	Lisa E. Winsor	44,405
William G. Gosz	27,787	Timothy J. Oyer	36,628	David Wolf	17,528
Lawrence M. Green	29,384	Edward F. Perlman	28,105	Douglas R. Wolf	36,971
George L. Greenfield	17,756	Michael J. Pomianek	46,190	Edward J. Russavage	43,069
James M. Hanifin, Jr.	39,213	Elizabeth R. Plumer	36,637		
Therese A. Hendricks	30,389	Randy J. Pritzker	35,986		
Steven J. Henry	27,900	Robert E. Rigby, Jr.	36,904		

48

Address all telephone calls to Lawrence M. Green at telephone no. (617) 720-3500. Address all correspondence to:

Lawrence M. Green
c/o Wolf, Greenfield & Sacks, P.C.,
Federal Reserve Plaza
600 Atlantic Avenue
Boston, MA 02210-2211

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

K E Thomas — 30/5/2001

Inventor's signature — **Date**

Full name of first or joint inventor: Kenneth Edwin Thomas
Citizenship: New Zealand
Residence: 20 Malabar Drive, Ellerslie, Auckland, New Zealand NZX
Post Office Address: 20 Malabar Drive, Ellerslie, Auckland, New Zealand

J Wm Hodgson — 30 May 2001

Inventor's signature — **Date**

Full name of second joint inventor: John William Nelson Hodgson
Citizenship: New Zealand
Residence: 2/18 Church Street, Northcote Point, Auckland, New Zealand NZX.
Post Office Address: 2/18 Church Street, Northcote Point, Auckland, New Zealand